HIDING THE RINGS:

THE IMPORTANCE OF P2P ENCRYPTION IN MONERO

Lee Clagett (@vtnerd)
Monerotopia 2022

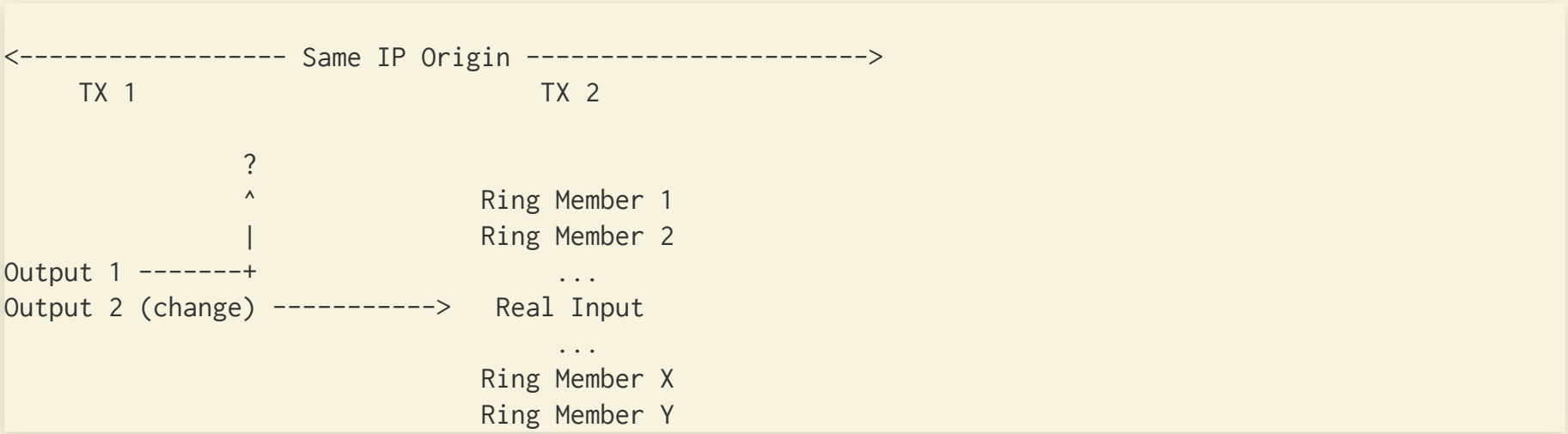
LEE CLAGETT (@VTNERD)

- Software Developer for Monero related projects since 2016
- Crowd-Funded Monero Developer Since ~2020

CRYPTOCURRENCY PRIVACY ISSUES (VERY HIGH LEVEL)

- Blockchain privacy
- TCP/IP privacy - failures cause:
  - Remote code execution!
  - Data dumps (heartbleed, log4j, etc.)
  - Coin tracking
    - Persistent surveillance can "break" rings if 2+ txes are observed

TCP/IP PERSISTENT SURVEILLANCE

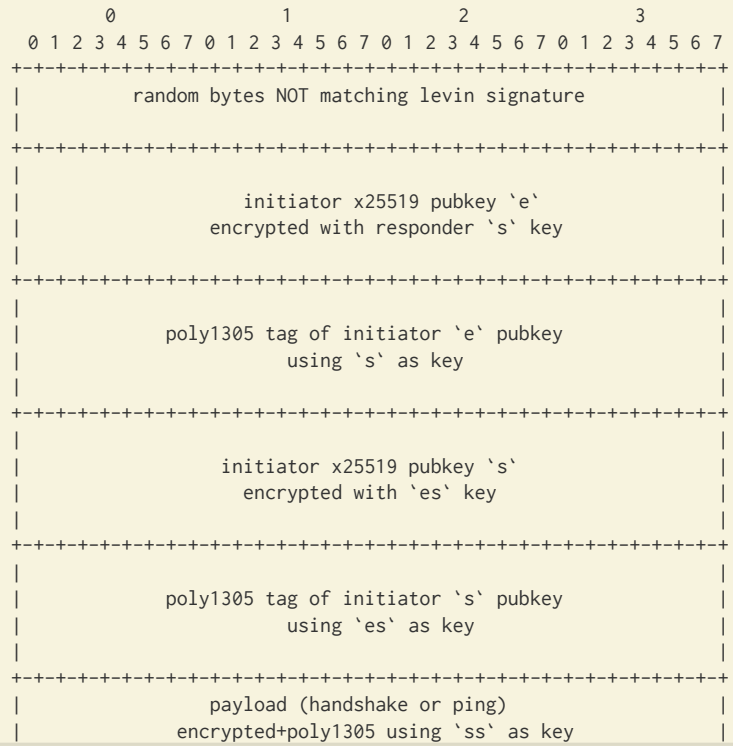


PROTECTING RINGS IN TRANSIT

- I2P/Tor
  - Protects against ISP and P2P Spies
- Dandelion++
  - Protects against P2P Spies
- P2P Noise Encryption
  - Protects* against ISP Spies

*I2P-like stealth connection headers instead of easily identifiable TLS headers

THE MONERO STEALTH P2P HEADER


0 1 2 3
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
random bytes NOT matching levin signature
initiator x25519 pubkey `e`
encrypted with responder `s` key
poly1305 tag of initiator `e` pubkey
using `s` as key
initiator x25519 pubkey `s`
encrypted with `es` key
poly1305 tag of initiator `s` pubkey
using `es` as key
payload (handshake or ping)
encrypted+poly1305 using `ss` as key

PROPERTIES OF THE P2P NOISE ENCRYPTION

- Default port numbers can easily identify Monero traffic
- Entire stream is random data and cannot be easily tracked by DPI engines
- If mandatory, old nodes will have to re-bootstrap

MOAR IMPLEMENTATION DETAILS

- No onion (I2P/Tor) routing
- Long-term static keys are shared in P2P init messages
- Long-term static keys are stored with IP/Port information
- Incorrect pubkey/IP/Port triplet is considered "soft" error
  - No authentication is performed on IP/port

HOW UPGRADE ENCRYPTION?

- Version number string is included in handshake key material
- Only 2 versions of encryption standard allowed per hardfork
- Receiver attempts to decrypt with newest version string then older

CONCERNS

- Custom encryption tech that doesn't completely "hide" Monero traffic
- Overhead (latency) of decryption slows block propagation slightly
- DoS mitigation is needed

QUESTIONS / COMMENTS

Ask about my wallet and project ideas after the talk!